James M. Fottrell

1400 New York Avenue N.W., 6th Floor
Washington, DC 20530
202-353-4721
James.M.Fottrell@usdoj.gov

Experience

Child Exploitation and Obscenity Section 2002 to Present
Criminal Division, U.S. Department of Justice Washington, DC

As Assistant to the Chief for Computer Forensics and Investigations, provide critical management of the High Technology Investigative Unit (HTIU) within the section to investigate child exploitation and obscenity offenses. Conduct forensic examinations of seized computers and storage media. Supervise forensic examinations conducted by three HTIU computer forensic specialists. Provide expert testimony in federal, state, and foreign courts in the area of computer forensics and Internet investigations. Provide technical guidance to federal, state, and international law enforcement agencies in support of large scale child exploitation investigations of commercial web sites, file servers, peer to peer software, instant messaging, and other emerging Internet technologies. Conduct technical training for attorneys and investigators in computer forensics and the various methods used to distribute child pornography and obscene materials. Manage all aspects of the HTIU Internet Investigation Network and Computer Forensics Network, including the Certification and Accreditation System Security Plan.

Customs Cybercrime Center 1997 - 2002
U.S. Customs Service Fairfax, VA
Under contract to the United States Customs Service, Office of Enforcement
Operation Artus (2002)
Provided a wide range of investigative support for an ongoing child exploitation case involving numerous subjects in the United States and in other countries. Responsible for setting up an Internet Relay Chat (IRC) client computer to help identify users based upon nicknames and screen aliases. Worked with agents and Internet Service Providers (ISPs) to identify individuals when traditional log records were not available. Responsible for writing programs, automated scripts, and other tools to parse through large volumes of log records and to extract relevant information.

Operation Buccaneer (August 2000 – July 2002)
Responsibilities included establishing various Internet based online covert identities and standardize techniques for case agents and analysts while using the Internet. Implemented covert web servers, email servers, domain name servers, and other Internet based machines to establish an authentic Internet presence. Worked with agents and United States Attorneys to establish procedures and policies for documenting online investigations including email messages, Internet Relay Chat (IRC) messages, and Web based content. Investigated and documented new and complex security mechanisms used to conceal participants' identity and location, including IRC servers, File Transfer Protocol (FTP) servers, and email encryption. Developed and implemented methods and techniques to identify and document illegal activity on the Internet. Provided technical expertise in archiving of information and backups of machines used for illegal activities including file servers, email servers, and other Internet based machines. Provided technical assistance to Assistant United States Attorneys in drafting Title III Wiretap orders for an Internet based electronic mail server. Worked with various technicians in the telecommunications industry to implement, process, and minimize captured messages on a Title III wiretap on a high speed network connection. Established policies and procedures to aide the forensic agents and analysts with the large volume of seized materials including materials from various systems including Microsoft Windows based systems and Unix system such as FreeBSD and Linux. Responsible for performing computer forensic examinations of seized material and extracting relevant material for case agents, analysts, and attorneys.

Provided testimony in Central Criminal Court in the United Kingdom regarding my activities related to identifying four UK defendants.

Operation Cheshire Cat (1998 – 1999)
Provided a wide range of computer support that resulted in thirty-two (32) federal searches in twenty-two (22) federal districts. Computer support included coordination of identifying targets of investigation, search warrants and forensic work both domestically and abroad. Testified in Federal Court (San Diego, CA 1/21/00) regarding computer evidence and Internet Relay Chat.

Computer Forensic Laboratory Support
Process requests from field offices to conduct forensic examinations of seized computer evidence and system administration of existing computer operating system including Microsoft Windows NT, Microsoft Windows 98, Sun Solaris, SunOS, HP-UX, SCO Unix, Linux, FreeBSD Unix, and Macintosh. Extensive programming development experience using C/C++, Unix, and PERL. Proficient in use of forensic software including Guidance Software’s Encase, Sydex Safeback, Access Data Forensic ForensicTool Kit, I-Look Investigator, ASR Expert Witness.

Office of Enforcement 1989 - 1994
U.S. Customs Service Washington, DC

As a project leader for the Office of Enforcement, responsibilities include managing a staff of ten consultants who provide support in the following areas: systems administration, computer forensics, database design and implementation, user support and training, and support for the IBM mainframe systems.

Systems administration responsibilities include adding and removing users from the system, daily, weekly and monthly backups to off-site storage, system tuning and optimization, security reviews, and networking between AT&T 3B2's, Pyramid 90x, and Novell and Banyan networks. Other duties include terminal, printer, and modem administration. Configured an OS/2 LAN Manager network to provide connectivity to several IBM mainframes for file transfers and 3270 terminal emulation. Installed a custom-built software package under OS/2 Presentation Manager to automatically convert mainframe data into an R:Base application.

Operation Longarm (1992)
Traveled to Denmark to work with Danish authorities in analyzing seized computer “BAMSE Bulletin Board System (BBS)”. Organized evidence and identified worldwide members including thirty-four (34) U.S. citizens. Provided training and support for Customs agents responsible for seizing and analyzing computer evidence.

Education

State University of New York, College at Oswego 1985
B.A. Computer Science, Minor: Mathematics Oswego, NY

Microsoft Certified Systems Engineer 1996

Encase Forensic Training 1999

Activities

High Technology Crime Investigation Association, Mid-Atlantic Chapter, 2005.
International Association of Computer Investigative Specialists, 1993.

Awards

Assistant Attorney General’s Award for Outstanding Advocacy in Protecting Citizens from Online Crime. 2008
Assistant Attorney General’s Award for Outstanding Advocacy in Protecting Citizens from

Online Crime. 2006
Attorney General's Award for Excellence in Information Technology,
U.S. Department of Justice, 2005
Certificate of Commendation, U.S. Department of Justice, Criminal Division, 2004
Exceptional Service in the Public Interest Award, Federal Bureau of Investigation, 2004
Special Achievement Award, U.S. Department of Justice, Criminal Division, 2003, 2004
Letter of Commendation, Attorney General's Award, U.S. Department. of Justice, 1999

Publications

Making a Child Exploitation Case with Computer Forensics, U.S. ATTORNEYS' BULLETIN, Vol. 52, No. 2, Mar. 2004, at 24, with Michelle Morgan-Kelly.

Selected Presentations

Technical Aspects of Child Pornography Investigation and Prosecution, International Cooperation in the Sphere of Child Trafficking and Child Pornography Conference, Moscow, Russia, Nov. 2008.

Who Did It? Pinning Down the Offender, Dallas Crimes Against Children Conference, Dallas, Texas, Aug. 2008.

Understanding Forensic Exams and Their Capacity to Build a Case, National Project Safe Childhood Conference, St. Louis, Missouri, Dec. 2007.

Working with Digital Evidence: Advanced Computer Forensics, National Internet Crimes Against Children Conference, San Diego, California, Oct. 2007.

Creeping the Web for Online Sharing Communities, Investigation and Prosecution Seminar, U.S. Department of Justice National Advocacy Center, Columbia, SC, Jul. 2006.

How the Internet is Misused by Pornographers, Obscenity Investigation and Prosecution Seminar, U.S. Department of Justice National Advocacy Center, Columbia, SC, Sep. 2005.

Internet Investigations, Obscenity Investigation and Prosecution Seminar, U.S. Department of Justice National Advocacy Center, Columbia, SC, Sep. 2005.

Computer Forensics, Forensics for Prosecutors Seminar, U.S. Department of Justice National Advocacy Center, Columbia, SC, Mar. 2005.

Advanced Search and Seizure Issues: Peer to Peer Operations, Advanced Child Exploitation Seminar, U.S. Department of Justice National Advocacy Center, Columbia, SC, Mar.2005.

Fighting High Technology Crime: Effectively Combating a Hacker Defense, Advanced Child Exploitation Seminar, U.S. Department of Justice National Advocacy Center, Columbia, SC, Mar. 2005.

Effective Computer Forensic Examination: What a Prosecutor Needs to Know, Fundamentals in the Prosecution of Child Exploitation Cases, U.S. Department of Justice National Advocacy Center, Columbia, SC, Aug. 2004.

Court Testimony
U.S. v. Richard Carino (2008)
U.S. v. Paul Little (2008)
U.S. v. Gregory Kapordelis (2007)
U.S.. v. Timothy Richards (2006)
U.S.. v. Donald Deverso (2006)
U.S.. v. Donald Anson (2006)
U.S.. v. Dwight Whorley (2005)
U.S. v. Michael Aaron O'Keefe (2004)
U.S. v. Richard Connors (2003)
U.S. v. Blazevich (1999)
U.S. v. Mohrbacher (1997)
U.S. v. Kimbrough (1994)
U.S. v. Lacy (1994)
Central Criminal Court, United Kingdom, (2003, 2004)